10

15

20

30



WE CLAIM:

1. A computer program product for controlling a computer, said computer program product comprising:

malware infection detecting logic operable to detect a malware infection of at least one computer; and

device disabling logic operable upon detection of said malware infection to disable operation of one or more data I/O devices of said at least one computer.

2. A computer program product as claimed in claim 1, wherein said malware infection detection logic detects a malware infection by one or more of:

positively identifying an item of malware upon said at least one computer; and identifying behaviour of said at least one computer indicative of malware infection.

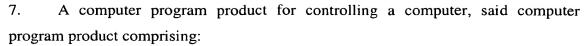
- 3. A computer program product as claimed in claim 1, wherein said one or more data I/O devices include one or more of:
 - a floppy disk drive;
 - a compact disk drive;
 - a removable media drive; and
 - a network interface card.
- 4. A computer program product as claimed in claim 1, wherein said device disabling logic is operable upon detection of malware infection to disable at least one data I/O device of at least one further computer.
 - 5. A computer program product as claimed in claim 1, wherein said device disabling logic is operable to require user confirmation prior to disabling said one or more data I/O devices.
 - 6. A computer program product as claimed in claim 1, wherein said device disabling logic is operable to disable said one or more data I/O devices using an API call to an operating system of said at least one computer.

10

20

25

30



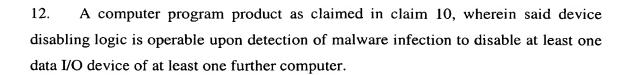
device disabling logic operable upon receipt by a computer of a command indicative of malware infection precautions being taken to disable operation of one or more data I/O devices of said computer.

- 8. A computer program product as claimed in claim 7, wherein said one or more data I/O devices include one or more of:
- a floppy disk drive;
 - a compact disk drive;
 - a removable media drive; and
 - a network interface card.
- 9. A computer program product as claimed in claim 7, wherein said device disabling logic is operable to disable said one or more data I/O devices using an API call to an operating system of said at least one computer.
 - 10. A computer program product for controlling a computer, said computer program product comprising:

user input logic operable to receive a user input indicative of activating precautions against a malware infection; and

device disabling logic operable upon receipt of said user input to disable operation of one or more data I/O devices of said at least one computer.

- 11. A computer program product as claimed in claim 10, wherein said one or more data I/O devices include one or more of:
 - a floppy disk drive;
 - a compact disk drive;
 - a removable media drive; and
 - a network interface card.



- 13. A computer program product as claimed in claim 10, wherein said device disabling logic is operable to disable said one or more data I/O devices using an API call to an operating system of said at least one computer.
- 14. A method of protecting against malware infection, said method comprising the steps of:

detecting a malware infection of at least one computer; and

upon detection of said malware infection disabling operation of one or more data I/O devices of said at least one computer.

15 15. A method as claimed in claim 14, wherein detection of a malware infection is by one or more of:

positively identifying an item of malware upon said at least one computer; and identifying behaviour of said at least one computer indicative of malware infection.

20

25

- 16. A method as claimed in claim 14, wherein said one or more data I/O devices include one or more of:
 - a floppy disk drive;
 - a compact disk drive;
 - a removable media drive; and
 - a network interface card.
- 17. A method as claimed in claim 14, wherein upon detection of malware infection at least one data I/O device of at least one further computer is disabled.

30

18. A method as claimed in claim 14, wherein user confirmation is required prior to disabling said one or more data I/O devices.

- 19. A method as claimed in claim 14, wherein disabling said one or more data I/O devices uses an API call to an operating system of said at least one computer.
- 20. A method of protecting against malware infection, said method comprising the steps of:

upon receipt by a computer of a command indicative of malware infection precautions being taken disabling operation of one or more data I/O devices of said computer.

- 10 21. A method as claimed in claim 20, wherein said one or more data I/O devices include one or more of:
 - a floppy disk drive;
 - a compact disk drive;
 - a removable media drive; and
- 15 a network interface card.
 - 22. A method as claimed in claim 20, wherein disabling said one or more data I/O devices uses an API call to an operating system of said at least one computer.
- 23. A method of protecting against malware infection, said method comprising the steps of:

receiving a user input indicative of activating precautions against a malware infection; and

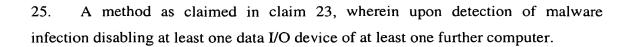
upon receipt of said user input disabling operation of one or more data I/O devices of said at least one computer.

- 24. A method as claimed in claim 23, wherein said one or more data I/O devices include one or more of:
 - a floppy disk drive;
- 30 a compact disk drive;
 - a removable media drive; and
 - a network interface card.

10

15

30



- 26. A method as claimed in claim 23, wherein disabling said one or more data I/O devices uses an API call to an operating system of said at least one computer.
 - 27. Apparatus for protecting against malware infection, said apparatus comprising:

a malware infection detector operable to detect a malware infection of at least one computer; and

a device disabling unit operable upon detection of said malware infection to disable operation of one or more data I/O devices of said at least one computer.

28. Apparatus as claimed in claim 27, wherein said malware infection detector detects a malware infection by one or more of:

positively identifying an item of malware upon said at least one computer; and identifying behaviour of said at least one computer indicative of malware infection.

- 29. Apparatus as claimed in claim 27, wherein said one or more data I/O devices include one or more of:
 - a floppy disk drive;
 - a compact disk drive;
 - a removable media drive; and
- a network interface card.
 - 30. Apparatus as claimed in claim 27, wherein said device disabling unit is operable upon detection of malware infection to disable at least one data I/O device of at least one further computer.
 - 31. Apparatus as claimed in claim 27, wherein said device disabling unit is operable to require user confirmation prior to disabling said one or more data I/O devices.

15

20

25

- 32. Apparatus as claimed in claim 27, wherein said device disabling unit is operable to disable said one or more data I/O devices using an API call to an operating system of said at least one computer.
- 5 33. Apparatus for protecting against malware infection, said apparatus comprising:
 - a device disabling unit operable upon receipt by a computer of a command indicative of malware infection precautions being taken to disable operation of one or more data I/O devices of said computer.
 - 34. Apparatus as claimed in claim 33, wherein said one or more data I/O devices include one or more of:
 - a floppy disk drive;
 - a compact disk drive;
 - a removable media drive; and
 - a network interface card.
 - 35. Apparatus as claimed in claim 33, wherein said device disabling unit is operable to disable said one or more data I/O devices using an API call to an operating system of said at least one computer.
 - 36. Apparatus for protecting against malware infection, said apparatus comprising:
 - a user input unit operable to receive a user input indicative of activating precautions against a malware infection; and
 - a device disabling unit operable upon receipt of said user input to disable operation of one or more data I/O devices of said at least one computer.
- 37. Apparatus as claimed in claim 36, wherein said one or more data I/O devices include one or more of:
 - a floppy disk drive;
 - a compact disk drive;
 - a removable media drive; and
 - a network interface card.

- 38. Apparatus as claimed in claim 36, wherein said device disabling unit is operable upon detection of malware infection to disable at least one data I/O device of at least one further computer.
- 39. Apparatus as claimed in claim 36, wherein said device disabling unit is operable to disable said one or more data I/O devices using an API call to an operating system of said at least one computer.